

IC CARD

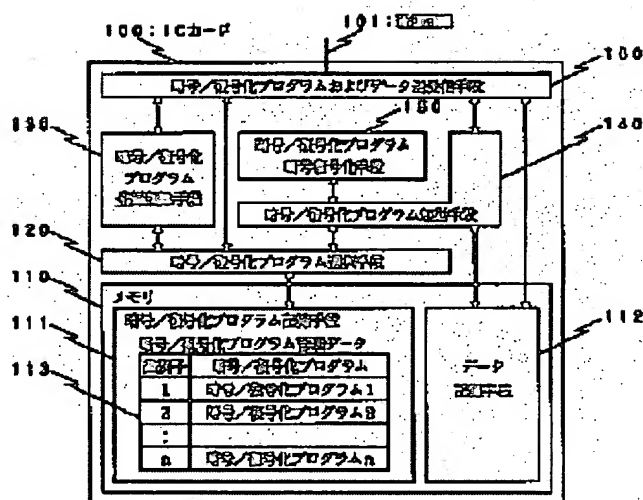
Patent number: JP11338993
Publication date: 1999-12-10
Inventor: OBANA MANABU; OKUHARA SUSUMU; TAKEYABU HIDEKI
Applicant: HITACHI LTD
Classification:
 - international: G06K19/073; G06K19/10
 - european:
Application number: JP19980149147 19980529
Priority number(s):

Report a data error here

Abstract of JP11338993

PROBLEM TO BE SOLVED: To improve the secrecy of enciphering/deciphering programs by transmitting and receiving enciphering/deciphering programs themselves to and from an external information processor or another IC card to eliminate the need of collectively holding enciphering/deciphering programs of all IC cards in an information processor.

SOLUTION: When there are reception data, the data kind of the header part of reception data is discriminated. Information to discriminate such kinds of data that is an enciphering program, a deciphering program, a complexing program or other data, is set in the data classification. If it is an enciphering/deciphering program, an identifier of the enciphering/deciphering program is read from reception data to confirm whether the enciphering/deciphering program corresponding to the designated identifier exists or not. An identifier which coincides with the identifier of the received enciphering/deciphering program is retrieved from enciphering/deciphering program management data 113. When a corresponding identifier is found, enciphering/deciphering program management data corresponding to the identifier is returned.



BEST AVAILABLE COPY

Data supplied from the **esp@cenet** database - Patent Abstracts of Japan

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-338993

(43) 公開日 平成11年(1999)12月10日

(51) Int.Cl.⁶

G 0 6 K 19/073
19/10

識別記号

F I

G 0 6 K 19/00

P

R

審査請求 未請求 請求項の数 6 O L (全 10 頁)

(21) 出願番号

特願平10-149147

(22) 出願日

平成10年(1998)5月29日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 尾花 学

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(72) 発明者 奥原 進

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

(72) 発明者 竹藪 英樹

神奈川県横浜市戸塚区戸塚町5030番地 株

式会社日立製作所ソフトウェア開発本部内

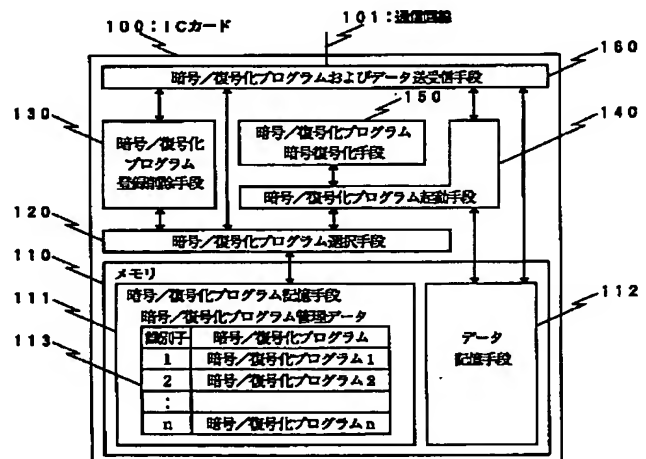
(74) 代理人 弁理士 矢島 保夫

(54) 【発明の名称】 ICカード

(57) 【要約】

【課題】プログラムに基づいた暗号および復号処理により送受信データを暗号化および復号化してICカードにデータを送受信するシステムにおいて、ICカード毎に異なる暗号化および復号化プログラムを使用することを容易にすると共に、ICカードへの送受信データの秘匿性の向上を可能にする。

【解決手段】送受信対象となるデータの暗号化および復号化を行なうプログラム(暗号/復号化プログラム)をICカード内に複数に記憶させる手段、任意の暗号/復号化プログラムを選択する手段、暗号/復号化プログラムを登録削除する手段、暗号/復号化プログラムを起動して送受信データを暗号あるいは復号化する手段、暗号/復号化プログラム自体を別の暗号/復号化プログラムで暗号化または復号化するための手段および暗号/復号化プログラムを送受信するための手段を備えたICカード。



【特許請求の範囲】

【請求項1】プログラムに基づいた暗号および復号処理により送受信データを暗号化するシステムで用いるICカードであって、

暗号化あるいは復号化プログラム（以後、暗号／復号化プログラムと記述する）を記憶するための暗号／復号化プログラム記憶手段と、

暗号／復号化プログラム記憶手段に記憶された暗号／復号化プログラムを起動させ、暗号化対象データを暗号データとし、または、復号化対象データを復号データとする、暗号／復号化プログラム起動手段と、

暗号／復号化プログラムにより暗号化したデータを送信するときに、データ受信元に対して事前にまたは同時に、暗号化したデータを解読するための暗号／復号化プログラムを送信および受信する暗号／復号化プログラム送受信手段と、

暗号／復号化プログラム記憶手段に対して暗号／復号化プログラムを登録および削除する暗号／復号化プログラム登録削除手段とを備えたことを特徴とするICカード。

【請求項2】前記暗号／復号化プログラム記憶手段は、前記暗号／復号化プログラムを複数記憶することを特徴とする請求項1に記載のICカード。

【請求項3】請求項2に記載の暗号／復号化プログラム記憶手段を備えるICカードにおいて、複数の暗号／復号化プログラムから任意の暗号／復号化プログラムを登録および削除する手段と、更に暗号／復号化プログラム起動手段において任意の暗号／復号化プログラムを起動する暗号／復号化プログラム選択手段を備えた請求項2に記載のICカード。

【請求項4】請求項3に記載の暗号／復号化プログラム選択手段において、ICカード内に記憶されている任意の暗号／復号化プログラムを識別するための識別手段を備え、識別子を指定することで、対応する暗号／復号化プログラムを起動する暗号／復号化プログラム起動手段を備えた請求項3に記載のICカード。

【請求項5】請求項1に記載した暗号／復号化プログラム自体を別の暗号化鍵または暗号化プログラムで暗号化する手段と、暗号化されたプログラムを暗号化した暗号化鍵に対応する復号化鍵または復号化プログラムで復号化する暗号／復号化プログラム暗号復号化手段を備えた請求項1から4の何れか1つに記載のICカード。

【請求項6】請求項1から5の何れか1つに記載のICカード、並びに、該ICカードに対して通信回線を介して任意の暗号／復号化プログラムを送信する手段と、送信した暗号／復号化プログラムのICカード内への登録要求手段と、ICカード内の任意の暗号／復号化プログラムの削除要求手段とを備えた情報処理装置を使用して、ICカードと情報処理装置間、または異なるICカード間で、通信回線を介して送受信するデータの暗号化および

復号化を行なうことを特徴とする暗号／復号化システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、プログラムに基づいた暗号および復号処理によりデータを暗号化および復号化するICカードに関する。

【0002】

【従来の技術】従来、データ（「情報」とも言う。）を秘匿するための手法として、暗号化鍵を用いて秘匿したいデータを暗号化する処理が知られている。データが一旦暗号化されると、暗号化で使った鍵と同一の鍵あるいは特定の復号化鍵を使用しないと解読できる状態に戻すことはできないため、そのような暗号化鍵や復号化鍵を所有していない人に対してデータを秘密にすることが可能である。

【0003】さらに、暗号化鍵や復号化鍵が漏洩すればデータが解読されてしまうことから、この暗号化鍵や復号化鍵に対して別の暗号化鍵にて暗号化して保管することにより安全性を高めてきた。

【0004】このようなシステムにおいてデータの暗号化処理あるいはデータ解読のための復号化処理は、情報処理装置にて暗号／復号化プログラムにより実行されるのが一般的である。この暗号／復号化プログラムによりデータが暗号化され、更に安全性を高めるために暗号化鍵まで暗号化することで、データの秘匿性を高めている。しかし、この暗号／復号化プログラム自体は、データ自体よりも無防備である事が多い。もしこのような暗号／復号化プログラムが第三者により解析されると、暗号化されたデータが解読されてしまう。または暗号／復号化プログラム自体を改竄し、第三者の知っている暗号化鍵にて暗号化する手段を付加することにより、その後、暗号化されたすべてのデータを第三者が解読することが可能になる恐れもある。

【0005】この暗号／復号化プログラムを第三者に改竄されることなく、かつ暗号化あるいは復号化を効率的に行うために、特開平9-6232号では、暗号／復号化プログラム自体を別の暗号化鍵で暗号化し、情報処理装置内の不揮発性メモリに格納し、情報処理装置からICカードに対してデータを送信する際に、暗号化された暗号／復号化プログラムをICカード内の揮発性メモリに送信し、ICカード内において当該プログラムを復号化した後に情報処理装置の揮発性メモリに送信し、復号化された暗号／復号化プログラムを用いて、送信するデータの暗号化あるいは復号化を行なっている。

【0006】

【発明が解決しようとする課題】しかし、このようなシステムにおいて、各ICカード毎に異なる暗号／復号化プログラムを使用する場合は、ICカードとデータを送受信する情報処理装置内に全てのICカードの暗号化さ

れた暗号／復号化プログラムを保有する必要があるため、膨大な記憶容量が要求されるという課題があった。

【0007】さらにICカード内で復号化した暗号／復号化プログラムを情報処理装置に送信する際、暗号／復号化プログラムは無防備な状態であり、送信中の暗号／復号化プログラムの漏洩の可能性が拡大するという課題がある。

【0008】本発明は、全てのICカードの暗号／復号化プログラムを情報処理装置内に一括保有する必要がある、暗号／復号化プログラムの秘匿性を向上させたICカードを提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するため、本発明は、暗号／復号化プログラムを記憶させる手段と、暗号／復号化プログラムを起動させる手段と、暗号／復号化プログラム自体を外部の情報処理装置または他のICカードに送受信する手段と、暗号／復号化プログラム登録削除手段をICカード内に備えることを特徴とする。

【0010】すなわち、請求項1に係る発明は、プログラムに基づいた暗号および復号処理により送受信データを暗号化するシステムで用いるICカードであって、暗号化あるいは復号化プログラム（以後、暗号／復号化プログラムと記述する）を記憶するための暗号／復号化プログラム記憶手段と、暗号／復号化プログラム記憶手段に記憶された暗号／復号化プログラムを起動させ、暗号化対象データを暗号データとし、または、復号化対象データを復号データとする、暗号／復号化プログラム起動手段と、暗号／復号化プログラムにより暗号化したデータを送信するときに、データ受信元に対して事前にまたは同時に、暗号化したデータを解読するための暗号／復号化プログラムを送信および受信する暗号／復号化プログラム送受信手段と、暗号／復号化プログラム記憶手段に対して暗号／復号化プログラムを登録および削除する暗号／復号化プログラム登録削除手段とを備えたことを特徴とする。

【0011】請求項2に係る発明は、請求項1において、前記暗号／復号化プログラム記憶手段は、前記暗号／復号化プログラムを複数記憶することを特徴とする。

【0012】請求項3に係る発明は、請求項2に記載の暗号／復号化プログラム記憶手段を備えるICカードにおいて、複数の暗号／復号化プログラムから任意の暗号／復号化プログラムを登録および削除する手段と、更に暗号／復号化プログラム起動手段において任意の暗号／復号化プログラムを起動する暗号／復号化プログラム選択手段を備えたことを特徴とする。

【0013】請求項4に係る発明は、請求項3に記載の暗号／復号化プログラム選択手段において、ICカード内に記憶されている任意の暗号／復号化プログラムを識別するための識別手段を備え、識別子を指定すること

で、対応する暗号／復号化プログラムを起動する暗号／復号化プログラム起動手段を備えたことを特徴とする。

【0014】請求項5に係る発明は、請求項1～4において、請求項1に記載した暗号／復号化プログラム自体を別の暗号化鍵または暗号化プログラムで暗号化する手段と、暗号化されたプログラムを暗号化した暗号化鍵に対応する復号化鍵または復号化プログラムで復号化する暗号／復号化プログラム暗号復号化手段を備えたことを特徴とする。

【0015】請求項6に係る発明は、請求項1から5の何れか1つに記載のICカード、並びに、該ICカードに対して通信回線を介して任意の暗号／復号プログラムを送信する手段と、送信した暗号／復号化プログラムのICカード内への登録要求手段と、ICカード内の任意の暗号／復号化プログラムの削除要求手段とを備えた情報処理装置を使用して、ICカードと情報処理装置間、または異なるICカード間で、通信回線を介して送受信するデータの暗号化および復号化を行なうことを特徴とする暗号／復号化システムである。

【0016】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態を説明する。

【0017】図2は、本発明の実施の形態のICカード100を構成するハード機構ブロック図である。このICカード100は、CPU210、入出力インタフェース(I/O)220、ROM230、RAM250、およびEEPROM240を備えている。ROM230は、記憶内容の読み出しは可能であるが記憶内容の更新ができない不揮発性のメモリを示す。RAM250およびEEPROM240は、共に記憶内容の読み出しならびに更新が可能であるが、RAM250はICカード100への電源供給が断たれると記憶内容を失う揮発性のメモリを示し、EEPROM240はICカード100への電源供給が断たれても記憶内容を失わない不揮発性のメモリを示す。

【0018】図1は、図2に示すICカード100内に本発明を実現するための各構成要素を配置したブロック図である。メモリ110は、図2のRAM250またはEEPROM240内に割り当てられた記憶領域を示す。秘密にしたいデータを暗号化あるいは暗号化されたデータを復号化するための暗号／復号化プログラムを記憶する暗号／復号化プログラム記憶手段111は、メモリ110内に割り当てられる。

【0019】また、ICカード100が受信したデータまたはICカード100内で処理するデータを記憶するためのデータ記憶手段112を、メモリ110内の暗号／復号化プログラム記憶手段111とは別の領域に割り当てる。

【0020】暗号／復号化プログラム記憶手段111内に記憶されている各暗号／復号化プログラムは、暗号／

復号化プログラム管理データ113によって管理する。図9は、暗号/復号化プログラム管理データの一実施例である。

【0021】ICカード100内の処理で任意の暗号/復号化プログラムを選択する場合、暗号/復号化プログラム選択手段120が暗号/復号化プログラム管理データ113を参照することで、指定された暗号/復号化プログラムを選択する。

【0022】任意の暗号/復号化プログラムを暗号/復号化プログラム記憶手段111に登録または暗号/復号化プログラム記憶手段111に既に登録されている任意の暗号/復号化プログラムを削除する場合、指定された暗号/復号化プログラムを暗号/復号化プログラム選択手段120により選択した結果を元に、暗号/復号化プログラム登録削除手段130によって暗号/復号化プログラム記憶手段111内の暗号/復号化プログラム管理データ113に管理データを登録すると共に指定された暗号/復号化プログラムをメモリ110内に組込む、または暗号/復号化プログラム管理データ113から対応する管理データを削除すると共に対応する暗号/復号化プログラムをメモリ110から削除する。

【0023】任意の暗号/復号化プログラムをICカード100内で起動する場合は、指定された暗号/復号化プログラムを暗号/復号化プログラム選択手段120により選択した結果を元に、暗号/復号化プログラム起動手段140によって指定された暗号/復号化プログラムを起動することで、データ記憶手段112内に記憶されている暗号化すべきデータの暗号化または復号化を行なう。

【0024】暗号/復号化プログラム起動手段140において、指定された暗号/復号化プログラムの暗号/復号化プログラム管理データ113内に暗号/復号化プログラム自体の復号化が必要なデータが格納されていた場合は、暗号/復号化プログラム暗号復号化手段150で指定された暗号/復号化プログラムを復号化してから暗号/復号化プログラム起動手段140によって起動する。

【0025】ICカード100において外部の情報処理装置からデータあるいは暗号/復号化プログラムを受信、または外部の情報処理装置にデータあるいは暗号/復号化プログラムを送信する場合は、暗号/復号化プログラムおよびデータ送受信手段160によって入出力インタフェース(I/O)220を使用して通信回線101へのデータの送受信を行う。

【0026】図1のブロック図において、暗号/復号化プログラム選択手段120、暗号/復号化プログラム登録削除手段130、暗号/復号化プログラム起動手段140、暗号/復号化プログラム暗号復号化手段150、並びに、暗号/復号化プログラムおよびデータ送受信手段160は、ICカード100内の不揮発性メモリであ

るROM230またはEEPROM240内に組込む。

【0027】以後、図1および図2に示した実施の形態のICカード100を使用した暗号化および暗号化データ転送の一例を、図3〜9に基づいて説明する。

【0028】図3は、ICカード100の入出力インタフェース(I/O)220を使用して通信回線101にデータ送信、または通信回線101からデータを受信するための暗号/復号化プログラムおよびデータ送受信手段160の処理を示す。本処理は、ICカード100が実行状態のときは常にデータ送受信の受け付けを可能にするため、S310およびS330の判定処理によって送受信データの有無の監視を行なう。

【0029】図8に、送受信するデータの形式を示す。受信データが有るときは、S340の処理で、受信データのヘッダー部のデータ種別を判定する。データ種別は、暗号化プログラム、復号化プログラム、またはデータであることを判定するための情報が設定されている。暗号/復号化プログラムならば、S350処理において受信データから暗号/復号化プログラムの識別子を読み取り、S400処理で指定識別子に対応する暗号/復号化プログラムの有無を確認する。

【0030】図4に、S400の暗号/復号化プログラム選択処理の流れを示す。暗号/復号化プログラム選択処理S400では、EEPROM240とRAM250内に設定されている暗号/復号化プログラム管理データ113から、受信した暗号/復号化プログラムの識別子と一致する識別子を検索する。対応する識別子が検出された場合は(S420)、その識別子に対応する暗号/復号化プログラム管理データをリターンし、検出できなかった場合は未登録としてエラーコードを設定して、S400処理コール元へリターンする。

【0031】S400処理で検索対象になる暗号/復号化プログラム管理データ113は、図9に示すような形式を構成している。暗号/復号化プログラムを識別するための識別子は、暗号/復号化プログラムを登録したカードIDとそのカード内で管理している暗号/復号化プログラムの番号から構成される。暗号/復号化プログラムの管理データは、暗号化プログラムのICカード100内の格納アドレス、ICカード100内の復号化プログラムの格納アドレス、そしてICカード100内に登録されているメモリ種別(EEPROMまたはRAMの別)、および登録されている暗号/復号化プログラムを実行する前に暗号/復号化プログラム自体を復号化する必要がある場合は、その復号化に使用する暗号/復号化プログラムの識別子(復号処理の欄)から構成されている。

【0032】図9に示した例では、自ICカード100のカードIDを「C001」とすると、自ICカードに登録した暗号/復号化プログラム識別子は「C00101」「C00102」の2種類であり(識別子は登録カ

ードIDとNoをつなげて表すものとする)、識別子が「C00102」である暗号/復号化プログラムは「C00101」によって暗号化されていることを表わしている。また暗号/復号化プログラム識別子「C02010」は、カードID「C020」からのデータ受信時にデータを復号化するための復号化プログラムの管理データのみが格納されていることを表す。さらに、暗号/復号化プログラム識別子「C00000」は、全ICカード共通に使用できるように、標準的にICカード100内に登録した暗号/復号化プログラムを表す。暗号/復号化プログラム識別子「C00101」や「C03011」は、この標準登録された「C00000」で暗号化されていることを表している。

【0033】再び図3に戻って、暗号/復号化プログラムおよびデータ送受信処理S300のS400処理で検索した結果を元に、S360処理で、受信データヘッダ一部より受信した暗号/復号化プログラムを登録するか削除するかを判定する。削除要求の場合は、暗号/復号化プログラム削除処理S500をコールして、指定暗号/復号化プログラムを削除した後、送信データの有無をチェックするS310から繰り返し処理を実行する。登録要求の場合は、S400処理の結果を元に、S370処理で受信した暗号/復号化プログラムが既に登録されているか判定し、未登録の場合は、暗号/復号化プログラム登録処理S500をコールする。S370処理で指定暗号/復号化プログラムが既に登録されていた場合、またはS500処理で新規に暗号/復号化プログラムをメモリ110内に登録した場合は、引き続き指定した暗号/復号化プログラム起動処理S600をコールし、引き続き、ICカード100が受信するデータの復号化処理を実行する。

【0034】S600処理で復号化されたデータは、S380処理で受信データを加工し、メモリ110に記憶させるなどの処理を実行した後、S310処理から繰り返し実行する。

【0035】図5に、前記S500処理の暗号/復号化プログラム登録および削除処理の流れを示す。まず、受信データヘッダ一部の暗号/復号化プログラムの登録(登録メモリ)または削除の領域を参照して、S510処理において、登録処理対象となる暗号/復号化プログラムの登録領域がEEPROM240かRAM250かを判定する。

【0036】登録削除対象がEEPROM240内の場合は、S520処理において登録または削除の判定を行ない、登録要求の場合は、S530処理においてEEPROM240内の暗号/復号化プログラム管理データに受信データから暗号/復号化プログラムの管理データを作成しEEPROM240内に格納する。削除要求の場合は、S540処理において、S400処理の結果を元にEEPROM240内の管理データと指定された暗号

/復号化プログラム自体を削除する。

【0037】登録削除対象がRAM250内の場合は、S550処理において、登録または削除の判定を行なう。登録要求の場合は、S560処理において、RAM250内の暗号/復号化プログラム管理データに受信したデータから暗号/復号化プログラムの管理データを作成しRAM250内に格納する。削除要求の場合は、意識的に削除処理は実行せずに、RAMの揮発特性を使用してICカード100に対する電源供給が断たれたときにRAM250内から管理データを削除(揮発)させる。

【0038】図6に、図3のS600の暗号/復号化プログラム起動処理の流れを示す。まず、対象となる暗号/復号化プログラムの識別子が例えば「C03011」の場合、プログラム自体を「C00000」プログラムで復号化するために、暗号/復号化プログラム暗号復号化処理S700をコールする。

【0039】図7に示すS700処理では、S710処理で、復号処理のための暗号/復号化プログラムの識別子(復号処理の欄)の有無を判定する。例えば「C03011」が指定されている場合は、「C00000」で復号化する必要があるため、当該識別子を使用して暗号/復号化プログラム選択処理S400をコールし、暗号/復号化プログラム管理データ情報を取得し、S700処理を再帰的にコールする。

【0040】再帰的にコールされたS700処理では、指定された識別子「C00000」の暗号/復号化プログラムを復号化する必要があるかどうかを、S710処理で判定する。「C00000」の暗号/復号化プログラムは復号する必要が無いのでそのままリターンする。

【0041】再帰的にコールしたS700処理からリターンされると、S710処理において識別子「C03011」の暗号/復号化プログラムは識別子「C00000」によって復号化され、S600処理へリターンする。

【0042】S700処理で復号化された識別子「C03011」の暗号/復号化プログラムを使用して、S610処理において、受信データヘッダ一部のデータ種別がデータで、復号化プログラムの識別子が「C03011」を指定してある受信したデータの復号化処理を実行する。

【0043】以後S380処理において受信したデータの参照、加工およびメモリ110への記憶、更新が可能になる。

【0044】ICカード100の受信データのデータ種別がデータの場合は、ヘッダ部に格納された復号化プログラムの識別子に従い、暗号/復号化プログラム起動処理S600をコールすることで、データの復号処理が実行される。

【0045】さらに、ICカード100の受信データの

データ種別がデータの場合で、ヘッダー部に復号化プログラムの識別子が格納されていない場合は、ICカード100が受信したデータは復号化の必要がない。

【0046】ICカードから暗号化したデータを送信する場合は、S600処理を使用し、暗号化対象データと暗号／復号化プログラムを指定し、S600処理においてデータを暗号化した後で、データ送信処理S320において、図8の形式に従ったデータ形式に変換して入出力インタフェース(I/O)220を介して通信回線上にデータを送信する。

【0047】本発明のICカード100に対して暗号／復号化プログラムの登録削除ならびにデータ送受信を外部情報処理装置から行なう場合は、図6、図7に記載した処理方式と図8に示したデータ形式に従った処理を行なうことで可能になる。

【0048】上記の実施形態により、秘匿したいデータの暗号化または復号化処理は、ICカード内に格納された暗号／復号化プログラムに依存することになり、さらに各ICカード毎に異なる暗号／復号化プログラムを搭載することが可能になる。

【0049】

【発明の効果】以上説明したように、本発明によれば、暗号／復号化プログラムを記憶させる手段と、暗号／復号化プログラムを起動させる手段と、暗号／復号化プログラム自体を外部の情報処理装置または他のICカードに送受信する手段と、暗号／復号化プログラム登録削除手段とを、ICカード内に備えるようにしているので、ICカードから外部の情報処理装置または他のICカードに暗号化したデータを送信する場合、送信するデータをICカード内に記憶されている暗号／復号化プログラムを使用して暗号化し、暗号化したデータの送信時または事前に暗号化したデータを復号化するため暗号／復号化プログラムを送信先に送信し、データを受信した情報処理装置または他のICカードは、受信した暗号／復号化プログラムを使用して受信した暗号化されたデータの復号化を行なうことが可能になる。これにより、各ICカード毎に異なる暗号／復号化プログラムをICカード内に保有することが可能になる。また、全てのICカードの暗号／復号化プログラムを情報処理装置内で一括保有することを不要にする。

【0050】またICカード内に暗号／復号化プログラ

ム自体を別の暗号化鍵または暗号化プログラムで暗号化する手段と、暗号化されたプログラムを暗号化した暗号化鍵に対応する復号化鍵または復号化プログラムで復号化する暗号／復号化プログラム暗号復号化手段を備えることで、ICカードから送信する暗号／復号プログラム自体を暗号化することを可能にし、送信中の暗号／復号化プログラムの秘匿性を向上することを可能にする。

【図面の簡単な説明】

【図1】本発明のICカード内に組込む手段のブロック図

【図2】本発明のICカードを構成するハード機構のブロック図

【図3】図1における暗号／復号化プログラムおよびデータ送受信手段の処理フローチャート図

【図4】図1における暗号／復号化プログラム選択手段の処理フローチャート図

【図5】図1における暗号／復号化プログラム登録削除手段の処理フローチャート図

【図6】図1における暗号／復号化プログラム起動手段の処理フローチャート図

【図7】図1における暗号／復号化プログラム暗号復号化手段の処理フローチャート図

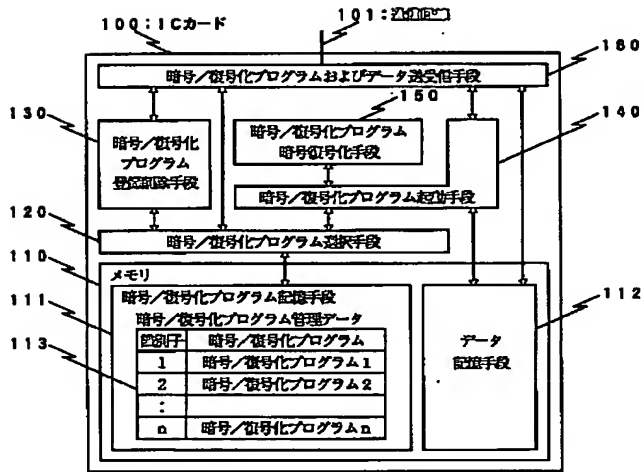
【図8】本発明のICカードが送受信するデータ形式例を示す図

【図9】図1における暗号／復号化プログラム記憶手段内部に格納する暗号／復号化プログラム管理データの例を示す図

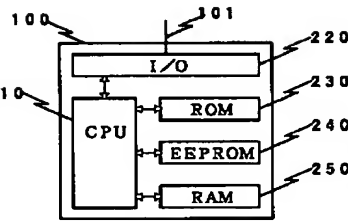
【符号の説明】

100：ICカード、101：通信回線（有線または無線の伝送路）、110：メモリ（EEPROMまたはRAMを示す）、111：暗号／復号化プログラム記憶手段、112：データ記憶手段、113：暗号／復号化プログラム管理データ、120：暗号／復号化プログラム選択手段、130：暗号／復号化プログラム登録削除手段、140：暗号／復号化プログラム起動手段、150：暗号／復号化プログラム暗号復号化手段、160：暗号／復号化プログラムおよびデータ送受信手段、210：CPU、220：入出力インタフェース(I/O)、230：ROM、240：EEPROM、250：RAM。

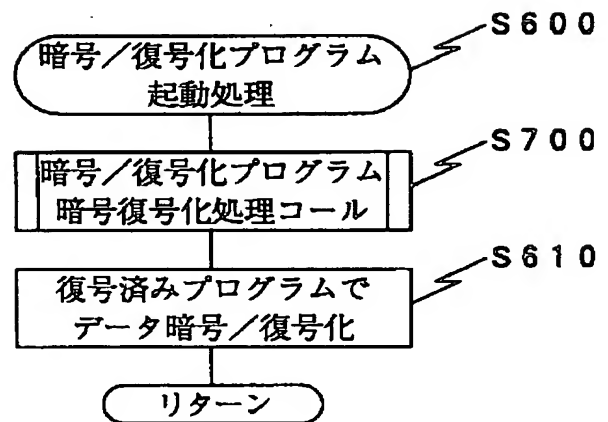
【図1】



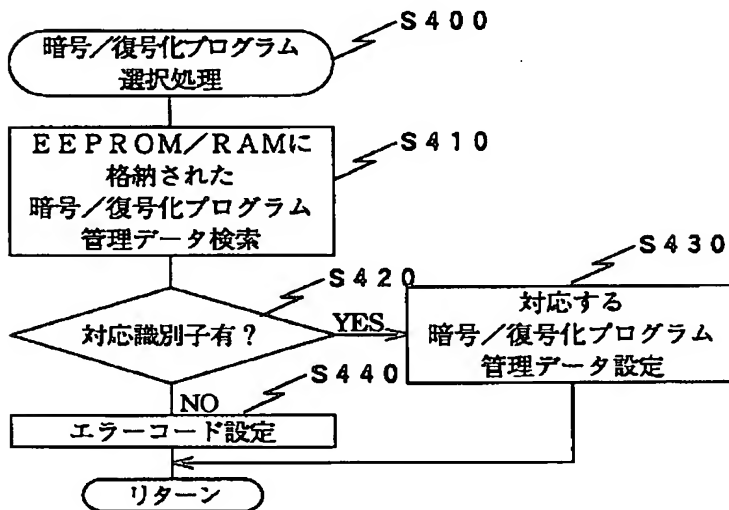
【図2】



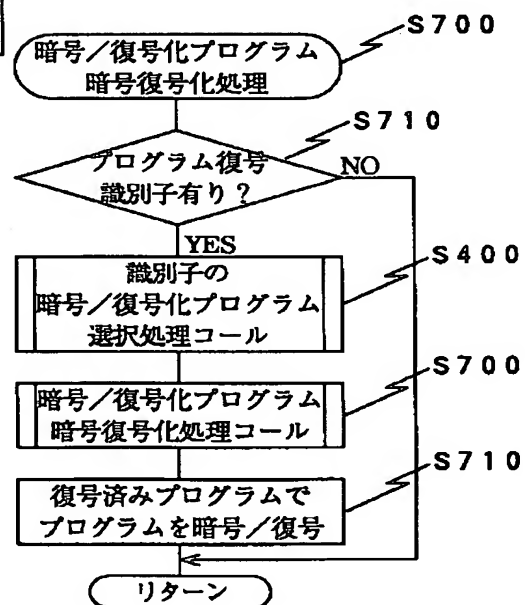
【図6】



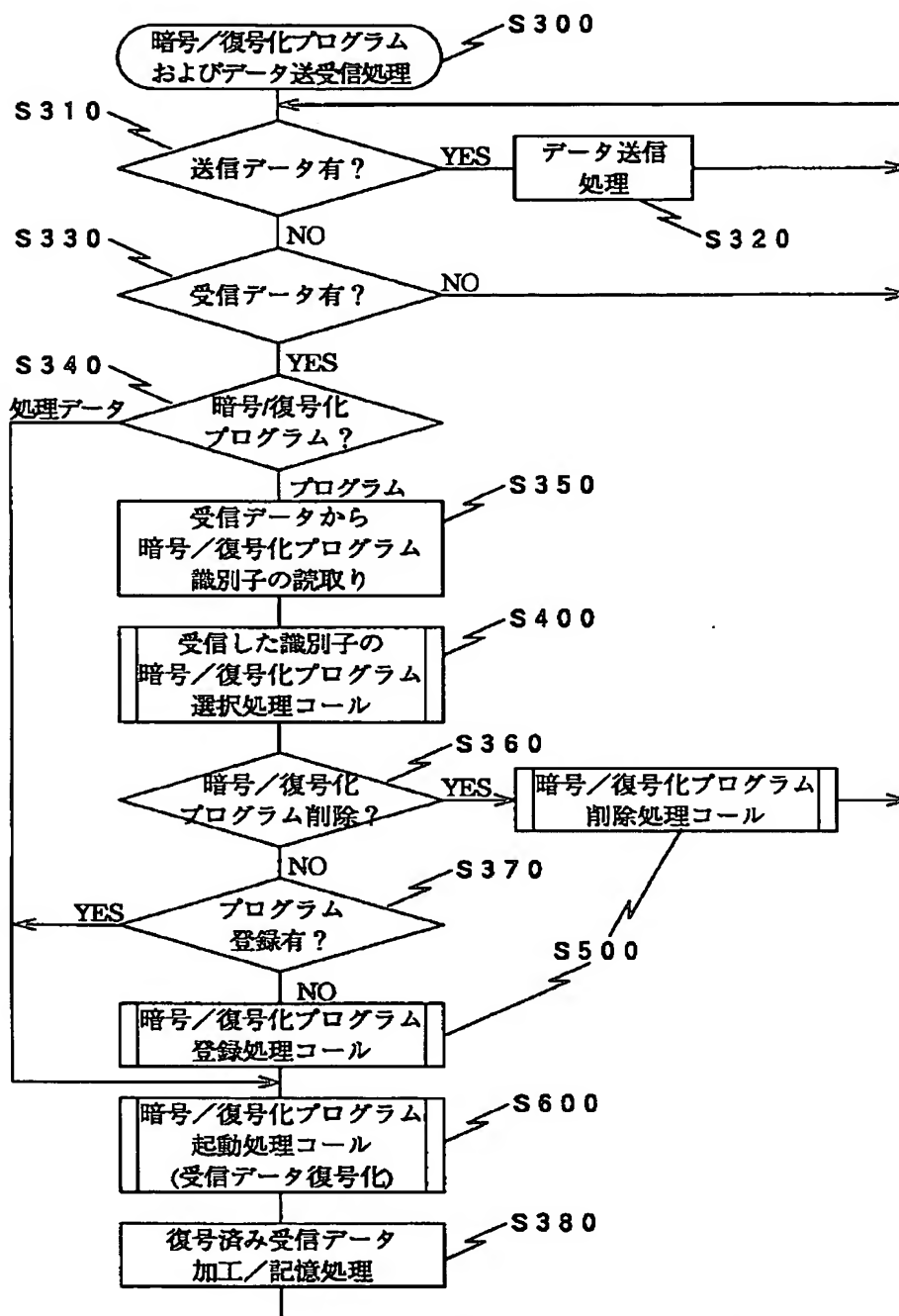
【図4】



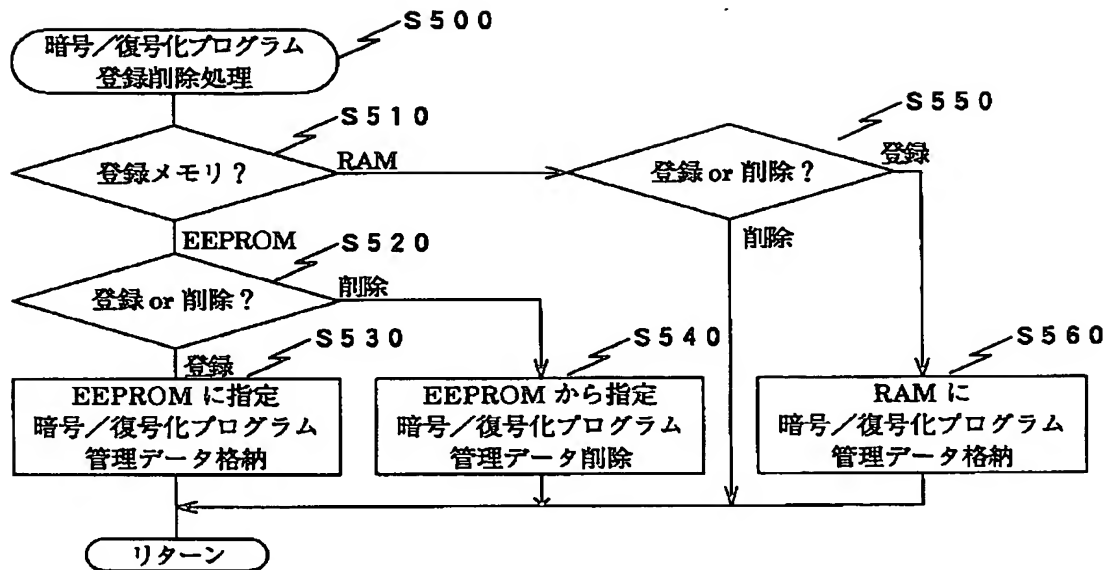
【図7】



【図3】



【図5】



【図8】

データ種別				
データの長さ				
ヘッダー部	プログラム時	暗号／復号化プログラムの識別子	データ時	復号化プログラムの識別子
		暗号／復号化プログラムの復号処理用の識別子		—
		暗号／復号化プログラムの登録（登録メモリ）または削除		—
データ部		暗号／復号化プログラム または データ		

【図9】

識別子		暗号／復号化プログラム				
登録カードID	No	暗号化 プログラム	復号化 プログラム	復号処理		送信先 登録メモリ
				登録カードID	No	
C000	00	アドレス	アドレス	—	—	—
C001	01	アドレス	アドレス	C000	00	EEPROM
C001	02	アドレス	アドレス	C001	01	RAM
⋮	⋮	⋮	⋮			
C020	10	—	アドレス	—	—	—
C030	11	—	アドレス	C000	00	—
⋮	⋮	⋮	⋮			

[JP,11-338993,A]

*** NOTICES ***

JPO and NCIP are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the IC card which enciphers and decrypts data by the code and decode processing based on a program.

[0002]

[Description of the Prior Art] The processing which enciphers data to keep it secret, using an encryption key as technique for keeping data (it also being called "information".) secret conventionally is known. Since it cannot return to the condition that it is decipherable if the key same once data are enciphered as the key used by encryption, or a specific decryption key is not used, it is possible to make data secret to those who own neither such an encryption key nor the decryption key.

[0003] Furthermore, if an encryption key and a decryption key are revealed, since data will be decoded, safety has been raised by enciphering and keeping it with another encryption key to this encryption key and decryption key.

[0004] As for the decryption processing for data encryption processing or data decode, in such a system, it is common that a code / decryption program performs with an information processor. The secrecy nature of data is raised because data are enciphered by this code / decryption program, and even an encryption key enciphers in order to raise safety further. However, this code / decryption program itself have that it is [much] more nearly defenseless than the data itself. A third person's analysis of such a code / a decryption program will decode the enciphered data. Or there is also a possibility of enabling a third person to decode all the enciphered data after that, by altering a code / the decryption program itself, and adding a means to encipher with the encryption key which the third person knows.

[0005] In order to perform encryption or a decryption efficiently, without a third person altering this code / decryption program, in JP,9-6232,A Encipher a code / the decryption program itself with another encryption key, and it stores in the nonvolatile memory in an information processor. In case data are transmitted from an information processor to an IC card, the enciphered code / decryption program are transmitted to the volatile memory in an IC card. After decrypting the program concerned in an IC card, it transmits to the volatile memory of an information processor, and the data encryption or decryption to transmit is performed using the decrypted code / decryption program.

[0006]

[Problem(s) to be Solved by the Invention] However, in such a system, since it was necessary to hold the code / decryption program as which all IC cards were enciphered in the information processor which transmits and receives an IC card and data to use different code / decryption program for every IC card, the technical problem that huge storage capacity was required occurred.

[0007] In case the code / decryption program furthermore decrypted within the IC card are transmitted to an information processor, a code / decryption program is in a defenseless condition, and has the technical problem that the possibility of leakage of the code / decryption program under transmission is expanded.

[0008] This invention does not have the need of carrying out package possession of the code / the decryption program of all IC cards into an information processor, and aims at offering the IC card which raised the secrecy nature of a code / decryption program.

[0009]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, this invention is characterized by having a means to make a code / decryption program memorize, a means to start a code / decryption program, a means to transmit and receive a code / the decryption program itself to an external information processor or other external IC cards, and a code / decryption program registration deletion means, in an IC card.

[0010] Namely, invention concerning claim 1 is an IC card used by the system which enciphers a transmitted and received data by the code and decode processing based on a program. The code / decryption program store means for memorizing encryption or a decryption program (it being henceforth described as a code / decryption program), Start the code / decryption program memorized by the code / decryption program store means, and the data for encryption are used as code data. Or when transmitting the data enciphered as the code / decryption program starting means which uses the data for a decryption as decode data by the code / decryption program As opposed to data receiving origin in advance Or the code / a decryption program transceiver means to transmit and receive the code / decryption program for decoding the data enciphered to coincidence, It is characterized by having the code / a decryption program registration deletion means to register and delete a code / decryption program to a code / decryption program store means.

[0011] Invention concerning claim 2 is characterized by said code / decryption program store means memorizing two or more said codes / decryption programs in claim 1.

[0012] It carries out having set invention concerning claim 3 to the IC card equipped with a code / decryption program store means according to claim 2, and having had a means register and delete the code / decryption program of arbitration from two or more code / decryption programs, and the code / decryption program selection means which starts the code / decryption program of arbitration in a code / decryption program starting means further as the description.

[0013] It carries out invention concerning claim 4 having been equipped with the discernment means for identifying the code / decryption program of the arbitration memorized in the IC card in a code / decryption program selection means according to claim 3, and having had the code / a decryption program starting means started the code / decryption program which is specifying an identifier and corresponds as the description.

[0014] Invention concerning claim 5 carries out having had a means encipher the code / the decryption program itself indicated to claim 1 by another encryption key or the encryption program, and the code / decryption program code decryption means decrypted by the decryption key or the decryption program corresponding to the encryption key which enciphered the enciphered program as the description in claims 1-4.

[0015] A means by which invention concerning claim 6 transmits the code / decode program of arbitration to the IC card of any one publication of five, and a list from claim 1 through a communication line to this IC card, The registration demand means into the IC card of the transmitted code / decryption program, The information processor equipped with the deletion demand means of the code / decryption program of the arbitration in an IC card is used. Between an IC card and an information processor or between different IC cards They are the code / decryption system characterized by performing the data encryption and decryption which are transmitted and received through a communication line.

[0016]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing.

[0017] Drawing 2 is a hard device block diagram which constitutes IC card 100 of the gestalt of operation of this invention. This IC card 100 is equipped with CPU210, an input/output interface (I/O) 220, and ROM230, RAM250 and EEPROM240. ROM230 shows the memory of the non-volatile which cannot perform renewal of the contents of storage, although read-out of the contents of storage is possible. Although read-out and updating of the contents of storage are possible for both RAM250 and EEPROM240, RAM250 shows the volatile memory which loses the contents of storage, when the current supply to IC card 100 is cut off, and shows the memory of the non-volatile in which EEPROM240 does not lose the contents of storage even if the current supply to IC card 100 is cut off. [0018] Drawing 1 is a block diagram which has arranged each component for realizing this invention in IC card 100 shown in drawing 2 . Memory 110 shows the storage region assigned in RAM250 or EEPROM240 of drawing 2 . The code / a decryption program store means 111 to memorize the code / decryption program for decrypting the data enciphered or enciphered in data to make it secret are assigned in memory 110.

[0019] Moreover, the data storage means 112 for memorizing the data processed within the data which IC card 100 received, or IC card 100 is assigned to field where the code / decryption program store means 111 in memory 110 are another.

[0020] Each code / decryption program memorized in the code / decryption program store means 111 are managed with a code / decryption program management data 113. Drawing 9 is one example of a code / decryption program management data.

[0021] When choosing the code / decryption program of arbitration by the processing in IC card 100, a code / decryption program selection means 120 chooses the specified code / decryption program by referring to a code / decryption program management data 113.

[0022] When the code / decryption program of the arbitration already registered into the code / decryption program store means 111 by registration, or the code / decryption program store means 111 in the code / decryption program of arbitration are deleted, The result of having chosen the specified code / decryption program with the code / decryption program selection means 120 to origin Incorporate the code / decryption program specified while registering

management data into the code / decryption program management data 113 within a code / decryption program store means 111 with the code / decryption program registration deletion means 130 in memory 110. Or the code / decryption program which corresponds while deleting the management data which corresponds from a code / decryption program management data 113 are deleted from memory 110.

[0023] When starting the code / decryption program of arbitration within IC card 100, it is starting the code / decryption program specified by the code / decryption program starting means 140 based on the result of having chosen the specified code / decryption program with the code / decryption program selection means 120, and the data encryption or the decryption which is memorized in the data-storage means 112 and which should be enciphered carries out.

[0024] In a code / decryption program starting means 140, when data [need / a code / the decryption program itself / to be decrypted] are stored in the code / decryption program management data 113 of the specified code / decryption program, after decrypting the code / decryption program specified with the code / decryption program code decryption means 150, it starts by the code / decryption program starting means 140. [0025] When transmitting data or a code / decryption program for data or a code / decryption program to the information processor of reception or the exterior from an external information processor in IC card 100, the data to a communication line 101 are transmitted and received with a code / decryption program, and the data transceiver means 160 using an input/output interface (I/O) 220. [0026] In the block diagram of drawing 1 , a code / decryption program, and the data transceiver means 160 are built into a code / decryption program selection means 120, the code / decryption program registration deletion means 130, the code / decryption program starting means 140, the code / decryption program code decryption means 150, and a list in ROM230 or EEPROM240 which is the nonvolatile memory in IC card 100.

[0027] Henceforth, an example of the encryption which used IC card 100 of the gestalt of operation shown in drawing 1 and drawing 2 , and encryption data transfer is explained based on drawing 3 -9.

[0028] Drawing 3 shows processing of the code / decryption program for receiving data from data transmission or a communication line 101 to a communication line 101 using the input/output interface (I/O) 220 of IC card 100, and the data transceiver means 160. This processing supervises existence of a transmitted and received data by judgment processing of S310 and S330 in order to always enable registration of data transmission and reception, when IC card 100 is a running state.

[0029] The format of the data transmitted and received to drawing 8 is shown. When there are received data, it is processing of S340 and the data classification of the header of received data is judged. The information for judging that data classification is an encryption program, a decryption program, or data is set up. If it is a code / decryption program, the identifier of a code / decryption program will be read in received data in S350 processing, and the existence of the code / decryption program corresponding to an assignment identifier will be checked by S400 processing.

[0030] The flow of the code / decryption program selection processing of S400 is shown in drawing 4 . The identifier of a code / decryption program which received, and an identifier in agreement are searched with a code / decryption program selection processing S400 from the code / decryption program management data 113 set up in EEPROM240 and RAM250. When a corresponding identifier is detected, the return of the code / the decryption program

management data corresponding to (S420) and its identifier is carried out, when undetectable, an error code is set up as un-registering, and a return is carried out to S400 processing call origin.

[0031] The code / decryption program management data 113 which becomes a candidate for retrieval by S400 processing constitute the format as shown in drawing 9 . The identifier for identifying a code / decryption program consists of numbers of the code / decryption program managed within the card ID which registered the code / decryption program, and its card. When a code / the decryption program itself needs to be decrypted before the management data of a code / a decryption program performs the code / the decode program which is registered into the storing address in IC card 100 of an encryption program, the storing address of the decryption program in IC card 100, and IC card 100 and which is registered [which are registered and is memory-classified (exception of EEPROM or RAM)], it consists of identifiers (the column of decode processing) of the code / the decryption program which uses to the decryption.

[0032] If the card ID of self-IC card 100 is set to "C001", the code / decryption program identifier registered with the self-IC card are two kinds, "C00101" and "C00102", (an identifier shall connect and express registration cards ID and No), and it expresses that the code / decryption program whose identifier is "C00102" are enciphered by "C00101" with the example shown in drawing 9 . Moreover, a code / decryption program identifier "C02010" means that only the management data of the decryption program for decrypting data is stored at the time of the data reception from Card ID "C020." Furthermore, a code / decryption program identifier "C00000" expresses the code / decryption program standardly registered into IC card 100 so that it can be used [all / IC card]. A code / decryption program identifier "C00101", and "C03011" mean being enciphered by these "C00000" by which standard registration was carried out.

[0033] It returns to drawing 3 again and judges [which registers the code / decryption program received from the received-data header by S360 processing based on the result searched with a code / decryption program, and Sdata transceiver processing S400 processing of 300 / or or] whether deletion is carried out. In a deletion demand, after calling a code / decryption program deletion S500 and deleting an assignment code / decryption program, repeat processing is performed from S310 which checks the existence of transmit data. In a registration demand, it judges whether the code / decryption program received by S370 processing are already registered based on the result of S400 processing, and, in not registering, a code / decryption program registration processing S500 is called. When the assignment code / decryption program is already registered by S370 processing, or when a code / decryption program is newly registered into memory 110 by S500 processing, the code / decryption program starting processing S600 specified succeedingly are called, and decryption processing of the data which IC card 100 receives is performed succeedingly.

[0034] The data decrypted by S600 processing process received data by S380 processing, and after they perform processing of making memory 110 memorize etc., they perform them repeatedly from S310 processing.

[0035] The flow of the code / decryption program registration of said S500 processing, and deletion is shown in drawing 5 . First, with reference to registration (registration memory) of the code / decryption program of a received-data header, or the field of deletion, the registration field of the code / decryption program used as a registration processing object judges EEPROM240 or RAM250 in S510 processing.

[0036] When the candidate for registration deletion is in EEPROM240, the judgment of registration or deletion is performed in S520 processing, in a registration demand, in S530 processing, the management data of a code / decryption program is created from received data to the code / decryption program management data in EEPROM240, and it stores it in EEPROM240. In a deletion demand, in S540 processing, the code / the decryption program itself specified as the management data in EEPROM240 based on the result of S400 processing are deleted.

[0037] When the candidate for registration deletion is in RAM250, the judgment of registration or deletion is performed in S550 processing. In S560 processing, in a registration demand, the management data of a code / decryption program is created from the data received to the code / decryption program management data in RAM250, and it stores it in RAM250. The case of a deletion demand makes management data delete from the inside of RAM250 intentionally, without performing deletion, when the current supply to IC card 100 is cut off using the volatilization property of RAM (volatilization).

[0038] The flow of the code / decryption program starting processing of drawing 3 of S600 is shown in drawing 6 . When the identifier of the target code / decryption program is "C03011", in order to decrypt the program itself by "C00000" program first, a code / decryption program code decryption processing S700 is called.

[0039] By S700 processing shown in drawing 7 , the existence of the identifier (column of decode processing) of the code / decryption program for decode processing is judged by S710 processing. For example, since it is necessary to decrypt by "C00000" when "C03011" is specified, a code / decryption program selection processing S400 is called using the identifier concerned, a code / decryption program management data information is acquired, and S700 processing is called recursively.

[0040] By S700 processing called recursively, it judges by S710 processing whether it is necessary to decrypt the code / decryption program of the specified identifier "C00000." Since there is no need of decoding, the return of the code / the decryption program of "C00000" is carried out as it is.

[0041] If a return is carried out from the S700 processing called recursively, in S710 processing, decoding of the code / the decryption program of an identifier "C03011" will be carried out by the identifier "C00000", and it will carry out a return to S600 processing by it.

[0042] The code / decryption program of the identifier "C03011" decrypted by S700 processing are used, and the data classification of a received-data header performs decryption processing of the received data in which the identifier of a decryption program specifies "C03011" by data, in S610 processing.

[0043] Reference of the data received in S380 processing after that, processing and the storage to memory 110, and updating are attained.

[0044] When the data classification of the received data of IC card 100 is data, according to the identifier of the decryption program stored in the header, it is calling a code / decryption program starting processing S600, and decode processing of data is performed.

[0045] Furthermore, when the identifier of a decryption program is not stored in the header by the case where the data classification of the received data of IC card 100 is data, the data which IC card 100 received do not have the need for a decryption.

[0046] When transmitting the data enciphered from the IC card, after using S600 processing, specifying the data for encryption, and a code / decryption program and enciphering data in S600 processing, in the data transmitting processing S320, it changes into the data format according to the format of drawing 8 , and data are transmitted on a communication line through an input/output interface (I/O) 220.

[0047] When performing registration deletion and data transmission and reception of a code / decryption program from an external information processor to IC card 100 of this invention, it becomes possible by performing processing according to the data format shown in mode of processing indicated to drawing 6 and drawing 7 , and drawing 8 .

[0048] It will depend for a data encryption or decryption processing to keep it secret on the code / decryption program stored in the IC card, and the above-mentioned operation gestalt enables it to carry further different the code / a decryption program for every IC card.

[0049]

[Effect of the Invention] A means to make a code / decryption program memorize as explained above according to this invention, A means to start a code / decryption program, and a means to transmit and receive a code / the decryption program itself to an external information processor or other external IC cards, Since he is trying to have a code / decryption program registration deletion means in an IC card When the data enciphered from the IC card to an external information processor or other external IC cards are transmitted, The data to transmit are enciphered using the code / decryption program memorized in the IC card. The information processor or other IC cards which transmitted the code / decryption program to the transmission place in order to decrypt the data enciphered the time of transmission of the enciphered data, or beforehand, and received data It becomes possible to decrypt the enciphered data which were received using the received code / decryption program. It enables this to hold different code / decryption program for every IC card in an IC card. Moreover, it makes it unnecessary to carry out package possession of the code / the decryption program of all IC cards within an information processor.

[0050] Moreover, it makes it possible to encipher in the code / the decode program itself transmit from an IC card by having a means encipher a code / the decryption program itself by another encryption key or the encryption program in an IC card, and the code / the decryption program code decryption means which decrypt by the decryption key or the decryption program corresponding to the encryption key which enciphered the enciphered program, and it makes it possible to improve the secrecy nature of the code / the decryption program under transmission.

[Claim(s)]

[Claim 1] It is the IC card used by the system which enciphers a transmitted and received data by the code and decode processing based on a program. The code / decryption program store means for memorizing encryption or a decryption program (it being henceforth described as a code / decryption program), Start the code / decryption program memorized by the code / decryption program store means, and the data for encryption are used as code data. Or when transmitting the data enciphered as the code / decryption program starting means which uses the data for a decryption as decode data by the code / decryption program As opposed to data receiving origin in advance Or the code / a decryption program transceiver means to transmit and receive the code / decryption program for decoding the data enciphered to coincidence, The IC card characterized by having the code / a decryption program registration deletion

means to register and delete a code / decryption program to a code / decryption program store means.

[Claim 2] Said code / decryption program store means are an IC card according to claim 1 characterized by memorizing two or more said codes / decryption programs.

[Claim 3] The IC card [equipped with a means to set to an IC card equipped with a code / decryption program store means according to claim 2, and to register and delete the code / decryption program of arbitration from two or more code / decryption programs, and the code / decryption program selection means which starts the code / decryption program of arbitration in a code / decryption program starting means further] according to claim 2.

[Claim 4] The IC card according to claim 3 which was equipped with the discernment means for identifying the code / decryption program of the arbitration memorized in the IC card in a code / decryption program selection means according to claim 3, and was equipped with the code / a decryption program starting means to start corresponding code / decryption program by specifying an identifier.

[Claim 5] The IC card of any one publication of four by claim 1 equipped with a means to encipher the code / the decryption program itself indicated to claim 1 by another encryption key or the encryption program, and the code / decryption program code decryption means decrypted by the decryption key or decryption program corresponding to the encryption key which enciphered the enciphered program.

[Claim 6] A means to transmit the code / decode program of arbitration to the IC card of any one publication of five, and a list from claim 1 through a communication line to this IC card, The registration demand means into the IC card of the transmitted code / decryption program, The information processor equipped with the deletion demand means of the code / decryption program of the arbitration in an IC card is used. Between an IC card and an information processor or between different IC cards The code / decryption system characterized by performing the data encryption and decryption which are transmitted and received through a communication line.

[Translation done.]

Japanese Publication for Unexamined Patent
Application No. 338993/1999 (Tokukaihei 11-338993)

[0033]

As shown in Fig. 3, based on a result obtained from the searching in the S400 process of the S300 for transmission/reception of encryption/decryption program and data, it is judged, from the received data-header section, whether the received encryption/decryption program is to be registered or deleted. If the deletion is requested, an encryption/decryption program deleting process S500 is called, to delete the designated encryption/decryption program is deleted. Then, the processes are repeated from the S310 which checks whether or not there is data to be transmitted. If the registration of the encryption/decryption program is requested, a S370 process is carried out to judge, based on the result obtained from the S400 process, whether or not the received encryption/decryption program has already been registered. If the encryption/decryption program is not registered, an encryption/decryption program registering process S500 is called. If (a) the encryption/decryption program has already been registered, or (b) the encryption/decryption program is newly registered to the memory 110 in the S500, an encryption/decryption program activating process S600 is called, the process S600 being for activating the designated encryption/decryption program. Then, a decrypting process is carried out with respect to data received by the IC card 100.

[0034]

After the data is decrypted in the process of the S600, the received data is processed in a S380. Then, a process such as storing of the data in the memory 110 is carried out, and the processes are repeated from the S310.

[0035]

Fig. 5 shows a flow of the encryption/decryption program registering/deleting process S500. First, in a S510 process, it is judged whether a registration area for the encryption/decryption program to be registered is the EEPROM 240 or the RAM 250, by referring to that portion of the received data-header section which indicates registration (registration memory) or deletion of the encryption/decryption program.

[0036]

If the encryption/decryption program to be registered or deleted is in the EEPROM 240, it is judged, in a S520 process, whether the encryption/decryption program is to be registered or deleted. If the registration is requested, a S530 process is carried out to create, from the received data, administrating data for the encryption/decryption program, the administrating data being created in the encryption/decryption program administrating data in the EEPROM 240. Then the encryption/decryption program administrating data is stored in the EEPROM 240. If the deletion is requested, a S540 process is carried out to delete (i) the administrating data in the EEPROM 240, and (ii) the designated encryption/decryption program itself, the deletion being carried out referring to the result of the S400 process.

[0037]

If the encryption/decryption program to be registered or deleted is in the RAM250, it is judged, in a S550 process, whether the encryption/decryption program is to be registered or deleted. If the registration is requested, a S560 process is carried out to create, from the received data, the administrating data for the encryption/decryption program, the administrating data being created in the encryption/decryption program administrating data in the RAM250. Then the encryption/decryption program administrating data is stored in the RAM250. If the deletion is requested, the deleting process is not deliberately carried out, and by using the volatile characteristic of the RAM, the administrating data is deleted (volatized) from the RAM250 when the power supply to the IC card 100 is stopped.

[0038]

Fig. 6 shows a flow of the encryption/decryption program activation process S600 shown in Fig. 3. For example, if the identifier of the targeted encryption/decryption program is "C03011", the encryption/decryption program encryption/decryption process S700 is called for decrypting the targeted encryption/decryption program by using a program whose identifier is "C00000".

[0039]

In the S700 process shown in Fig. 7, it is judged, in a S710 process, whether or not there is the identifier (in the column of "decrypting process") of the encryption/decryption program for use in the decrypting

process. For example, if "C03011" is designated, the program whose identifier is "C00000" is needed for the decrypting process. Accordingly, the encryption/decryption program selecting process S400 is called by using the identifier, thereby obtaining the encryption/decryption administrating data. Then, S700 process is recursively called.

[0040]

In the S700 being recursively called, it is judged, in the S710 process, whether or not it is necessary to decrypt the encryption/decryption program whose identifier is the designated identifier of "C00000". Since it is not necessary to decrypt the encryption/decryption program whose identifier is "C00000", the decrypting process is not carried out, and the process is returned.

[0041]

If the process is returned from the S700 having been recursively called, the encryption/decryption program whose identifier is "C00301" is decrypted by using the encrypting decrypting program whose identifier is "C00000". Then, the process is returned to S600 process.

[0042]

In a S610 process, the encryption/decryption program, whose identifier is "C00301", and which has been decrypted in the S700 process, is then used for decrypting received data whose data-header section indicates that the type of the received data is "data", and whose identifier of the decrypting program designates "C003011".

[0043]

After that, in the S380 process, it becomes possible to (i) refer to the received data, (ii) process the received data, (iii) store the received data in the memory 110, or (iv) update the received data having been stored.

[0044]

Thus, in a case where the type of the data received by the IC card 100 is the “data”, the encryption/decryption program activation process S600 is called, referring to the identifier of the decryption program, the identifier stored in the header section of the data, thereby the decrypting process of the data is carried out.

[0045]

Further, in a case where the type of the data received by the IC card 100 is the “data”, and the header section does not contain the identifier of the decrypting program, the data received by the IC card 100 does not have to be decrypted.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.